Opening Statement of the Honorable Mary Bono Mack
Subcommittee on Commerce, Manufacturing, and Trade
"Internet Privacy: The Impact and Burden of EU Regulation"
September 15, 2011
(As Prepared for Delivery)

Today, as we continue our series of hearings on Internet privacy, we are going to take a close look at the impact of regulations on commerce, consumers and businesses. As Chairman of this Subcommittee – I am guided by one critically important question: when it comes to the Internet, how do we balance the need to remain innovative with the need to protect privacy?

As someone who has followed this issue very closely over the years – and someone who, frankly, remains skeptical right now of both industry and government – I will continue to keep an open mind as to whether new legislation or regulations are warranted.

But let me be clear about one thing: to date, I do not believe industry has proven that it's doing enough to protect American consumers, while government, unfortunately, tends to overreach every time it gets involved in the marketplace. From my perspective, there's a sweet spot between too much regulation and no regulation at all. My goal is to find that sweet spot.

Today, the Internet pretty much remains a work in progress, even though it serves billions of users worldwide. And while e-commerce in the United States will top $200 billion this year for the first time, there's still a Wild, Wild West feel to cyberspace, leaving many consumers wondering if there's a Sheriff in town or whether they're completely on their own when it comes to protecting themselves and their families.

In just 25 years, the Internet has spurred sweeping, transformative innovations. It has become embedded in our daily lives. And it has unlimited potential to affect positive social and political change. Yet every single day, millions of Americans are subject to privacy threats. Most of them, by and large, are seemingly innocent – such as the collection of information about consumer buying habits – but some of them are malicious and criminal, often involving online theft and fraud.

This Subcommittee has a responsibility – and a unique opportunity, as well – to ferret out those differences and to do everything we can to keep the Internet free, while keeping consumers free, to the extent possible, from widespread privacy abuses.

I, for one, do not subscribe to the theory that "privacy is dead – get over it." There are smart ways to protect consumers and to allow e-commerce to continue to flourish. That's the sweet spot we should be searching for in our hearings. Additionally, I will continue to work with Members of both sides of the aisle to secure passage this year of the SAFE Data Act, which will provide American consumers with important new privacy safeguards.

Today, we are taking a close look at the European Union's Data Privacy Directive, first adopted on October 24, 1995. The EU model is one of the largest regulatory regimes in the world. I believe this hearing will be instructive, allowing us to better understand some of the "lessons learned" over the past 15-plus years. Clearly, there have been some unintended consequences as a result of the Directive which have proven problematic for both consumers and businesses.

The purpose of the Directive is to harmonize differing national legislation on data privacy protections within the European Union, while preventing the flow of personal information to countries that – in the opinion of EU regulators – lack sufficient privacy protections.

But as we will learn today, there has been no shortage of unintended consequences. In a way, you could say the EU Directive at some point crossed paths with Murphy's Law. Anything that can possibly go wrong, does.

Unfortunately, in all too many cases, it's gone wrong for American businesses trying to navigate these tricky regulations.

The Directive requires all EU member states to enact national privacy legislation which satisfies certain baseline privacy principles, ranging from notice to consent to disclosure to security. While these principles are the basis for the Directive, each EU member state is responsible for incorporating these articles into its own national privacy laws. This, in turn, has led to inconsistent regulatory regimes throughout the EU and has created serious problems for American multinational firms.

Making matters worse, compliance within the EU remains fractured, with several member states not fully complying with the Directive. This has led to sporadic and inconsistent enforcement, with a seemingly disproportionate number of American companies targeted for compliance violations.

Let me be clear: my purpose in holding this hearing is not to point fingers. Instead, my goal is to point to a better way to protect privacy online and promote e-commerce. In the end, this will benefit both American consumers and American businesses, and preserve a strongly-held belief all across America that the Internet should remain free.

###